

Opis Przedmiotu Zamówienia – część numer 1

Dostawa sprzętu IT i oprogramowania na rzecz Gminy Kunów

1. Serwer wraz z oprogramowaniem do wirtualizacji.

1. Serwer wraz z oprogramowaniem do wirtualizacji.

a) Serwer – 2 sztuki.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	- Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. - Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. - Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	- Płyta główna z możliwością zainstalowania do dwóch procesorów. - Obsługa procesorów 32 rdzeniowych. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. - Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie

	www.spec.org dla konfiguracji dwuprocessorowej.
RAM	Minimum 256GB DDR5 RDIMM 4800MT/s.
Funkcjonalność pamięci RAM	- Demand Scrubbing. - Patrol Scrubbing. - Permanent Fault Detection (PFD).
Gniazda PCI	Min. dwa sloty PCIe.
Interfejsy sieciowe/FC/SAS	- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. - Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe).
Dyski twarde	Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Wbudowane porty	4x USB, w tym min. 1 porty USB 3.0. 2x port VGA (jeden na panelu przednim). - Możliwość rozbudowy o Serial Port.
Video	Zintegrowana karta graficzna umożliwiającą wyświetlenie rozdzielczości min. 1280x1024.
Wentylatory	Redundantne, Hot-Plug.
Zasilacze	Redundantne, Hot-Plug min. 1100W klasy Titanium.
Bezpieczeństwo	- Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0. - Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in.

	prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera; ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera; oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej; ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym; ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze; ○ Automatyczna rejestracja certyfikatów (ACE).
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; ○ integracja z Active Directory; ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish; ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; ○ Szczegółowy opis wykrytych systemów oraz ich komponentów; ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF; ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu; ○ Grupowanie urządzeń w oparciu o kryteria użytkownika; ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji; ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; ○ Szybki podgląd stanu środowiska; ○ Podsumowanie stanu dla każdego urządzenia;

	- o Szczegółowy status urządzenia/elementu/komponentu; - o Generowanie alertów przy zmianie stanu urządzenia; - o Filtry raportów umożliwiające podgląd najważniejszych zdarzeń; - o Integracja z service desk producenta dostarczonej platformy sprzętowej; - o Możliwość przejęcia zdalnego pulpitu; - o Możliwość podmontowania wirtualnego napędu; - o Kreator umożliwiający dostosowanie akcji dla wybranych alertów; - o Możliwość importu plików MIB; - o Przesyłanie alertów „as-is” do innych konsol firm trzecich; - o Możliwość definiowania ról administratorów; - o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów; - o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); - o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta; - o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; - o Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera; - o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności; - o Wdrażanie serwerów, rozwiązań modularnych oraz przetłączników sieciowych w oparciu o profile; - o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami; - o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta; - o Zdalne uruchamianie diagnostyki serwera; - o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym; - o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001. • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty

	zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	- Zamawiający wymaga dokumentacji w języku polskim lub angielskim. - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. - Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych). - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. - Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. - Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. - Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
- Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
- Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
 - Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
 - Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
 - Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
 - Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
 - Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaze dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
- Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

b) Oprogramowanie serwerowe – 2 sztuki.

Licencje systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core.

Licencje systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

RÓWNOWAŻNOŚĆ:

1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter, Zamawiający wymaga dostarczenia licencji dla obecnych serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsługiwać serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
22. Możliwość wykorzystania standardu http/2.
23. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
26. Mechanizmy logowania w oparciu o: a) login i hasło,
 - a. karty z certyfikatami (smartcard),
 - b. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
 - a. określonych grup użytkowników,
 - b. zastosowanej klasyfikacji danych,
 - c. centralnych polityk dostępu w sieci,
 - d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
 - a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
 - b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
 - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
 - c. zdalna dystrybucja oprogramowania na stacje robocze,
 - d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
 - e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http,
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - f. szyfrowanie plików i folderów,

- g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
- h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
- i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
- j. serwis udostępniania stron WWW,
- k. wsparcie dla protokołu IP w wersji 6 (IPv6),
- l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
- n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- p. mechanizmy wirtualizacji mające wsparcie dla:
 - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - obsługi 4-KB sektorów dysków,
 - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
 - możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
- q. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
- r. wsparcie dla rozwiązania Kubernetes.
- s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiające lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- u. mechanizmy deduplikacji i kompresji na wolumenach.
- v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- w. mechanizm konfiguracji połączenia VPN do platformy Azure.
- x. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
- y. mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów.
- z. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

c) Licencje dostępne na użytkownika – 50 sztuk.

- 1. Licencje dostępne na użytkownika 50 sztuk.
 - Wymagana licencja typu Cal User OEM do systemu Windows Server 2022 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.

2. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2022 na użytkownika:

- Licencja dostępowa dla użytkownika umożliwiająca połączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu User Cal z wdrożoną rolą Active Directory.

2. Zarządzalne urządzenia sieciowe z obsługą VLAN – 6 sztuk

Lp.	Minimalne wymagania Zamawiającego	
I.	CECHY ZARZĄDZANIA	
1.	Typ przełącznika	Zarządzany
2.	Przełącznik wielowarstwowy	L2/L3
3.	Obsługa jakości serwisu (QoS)	Tak
4.	Zarządzany w chmurze	Tak
5.	Zarządzanie przez stronę www	Tak
6.	Inspekcja ARP	Tak
7.	Konfigurowanie ustawień lokalizacji (CLI)	Tak
8.	Obsługa MIB	Y
II.	OCHRONA	
9.	Funkcje DHCP	DHCP relay, DHCP server, DHCPv6 client
10.	Lista kontrolna dostępu (ACL)	Tak
11.	Zasady Listy Kontroli Dostępu (ACL)	1024
12.	IGMP snooping	Tak
13.	Ochrona hasłem	Tak
14.	obsługuje SSH/SSL	Tak
15.	Filtrowanie adresów MAC	Tak
16.	Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS
III.	PORTY I INTERFEJSY	

17.	Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48
18.	Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
19.	Ilość slotów Modułu SFP+	4
20.	Liczba portów USB 2.0	1
IV.	SIEĆ	
21.	Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad
22.	Obsługa 10G	Tak
23.	Dublowanie portów	Tak
24.	Protokół drzewa rozpinającego	Tak
25.	Blokowanie head-of-line (HOL)	Tak
26.	Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
27.	Kontrola wzrostu natężenia ruchu	Tak
28.	Automatyczne MDI/MDI-X	Tak
29.	Podpora kontroli przepływu	Tak
30.	Agregator połączenia	Tak
31.	Obsługa sieci VLAN	Tak
32.	Liczba VLANs	4094
V.	PRZESYŁANIE DANYCH	
33.	Wielkość tabeli adresów	16000 wejścia
34.	Zgodny z Jumbo Frames	Tak
35.	Rozszerzenie Jumbo Frames	9000
VI.	FUNKCJE MULTICAST	
36.	Obsługa Multicast	Tak
VII.	PROTOKOŁY	
37.	Protokoły zarządzające	SNMP

VIII.	KONSTRUKCJA	
38.	Możliwości montowania w stelażu	Tak
39.	Przycisk reset	Tak
40.	Diody LED	Tak
IX.	WYDAJNOŚĆ	
41.	Procesor wbudowany	Tak
42.	Taktowanie procesora	800 MHz
43.	Pojemność pamięci wewnętrznej	512 MB
44.	Wielkość pamięci flash	256 MB
45.	Aktualizacje oprogramowania urządzenia	Tak
X.	MOC	
46.	Zasilacz dołączony	Tak
XI.	WARUNKI PRACY	
47.	Zakres temperatur (eksploatacja)	-5 - 50 °C
48.	Zakres temperatur (przechowywanie)	-25 - 70 °C
49.	Zakres wilgotności względnej	10 - 90%
50.	Dopuszczalna wilgotność względna	10 - 90%

3. Zarządzalne urządzenia sieciowe z obsługą VLAN – 2 sztuki

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

- Ilość portów 8 portów SFP+ oraz 8 portów 10GbBaseT niezależne
- Chłodzenie od przodu do tyłu obudowy
- Tablica MAC min. 16K
- Tablica ARP/NDP min. 888
- Bufor 16Mb
- MTBF min. 196120 godzin
- Wydajność min. 238 Mp/s
- Przepustowość min. 320 Gb/s
- Port USB
- Port miniUSB

- Port zarządzania Out-of-band
- Web GUI
- HTTPs
- CLI
- Telnet
- SSH
- SNMP
- MIB RSPAN
- Radius
- TACACS+
- DiffServ
- Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
- IPv4/IPv6 Multicast filtering
- IGMPv3 MLDv2 Snooping
- ASM & SSM
- IGMPv1,v2 Querier
- Auto-VoIP
- Auto-iSCSI
- Policy-based routing (PBR)
- LLDP-MED
- Spanning Tree
- Green Ethernet
- STP
- MTP
- RSTP
- PV(R)STP
- BPDU/STP Root Guard
- IEEE (802.3az)
- GVRP/GMRP
- Q in Q
- Private VLAN
- DOT1X
- MAB
- Captive Portal
- DHCP Snooping
- Dynamic ARP
- Inspection
- IP Source Guard
- CPU min 800 Mhz
- Min 1GB RAM
- Min 256MB Flash
- Min ilość obsługiwanych VLAN 4K
- DHCP Server min 2K rezerwacji
- sFlow
- Minimalna ilość przełączników w stosie: 8
- Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
- Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
- Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
- Non-stop forwarding (NSF)
- Distributed Link Aggregation (LAGs across the stack)

- Ilość interfejsów IP 128
- Double VLAN Tagging (QoQ)
- Yes
- PIM-DM (Multicast Routing - dense mode)
- PIM-DM (IPv6)
- PIM-SM (Multicast Routing - sparse mode)
- PIM-SM (IPv6)
- RIPv1
- RIPv2
- OSPFv2
- RFC 2328
- RFC 1583
- OSPFv3
- OSPFv2 min. sąsiadów 400
- OSPFv3 min. sąsiadów 400
- OSPFv3 min. sąsiadów na interfejs 100
- UDLD
- LLPF
- DHCPv6 Snooping
- wysyłanie alertów na email
- MMRP
- Ilość ACL min. 100
- Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu

4. Macierz dyskowa – 1 sztuka

Element konfiguracji/cecha/funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5"
Przestrzeń dyskowa	Zainstalowane: 6x dysk SAS o pojemności min. 2.4TB, Hot-Plug 6x dysk NLSAS o pojemności min. 16TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardej.
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem

	wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów iSCSI 25Gb (4 porty na kontroler).
Kable/wkładki	4x kabel DAC 25GbE SFP28-SFP28 min. 5m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe

	licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności

	dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który spowodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN

	62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta

	sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
--	--

5. Serwer NAS – 2 sztuki

Minimalne wymagania Zamawiającego	
Typ urządzenia	Serwer NAS
Obudowa	Rack
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz (maksymalnie 2,7 GHz z technologią Turbo Boost)
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 8 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 64 GB
Możliwości rozbudowy	- Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 16 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń Infiniband - Wbudowane 2 gniazda M.2 obsługujące dyski SATA/NVMe
Porty zewnętrzne	Minimum: 2 porty USB 3.0 1 gniazdo rozszerzenia
Porty sieciowe	Minimum: 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 8-liniowe gniazdo x8
Wentylator obudowy	Min. 2 wentylatory (40 × 40 × 28 mm)

Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: - Wewnętrzny: Btrfs, ext4 - Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+
Zarządzanie pamięcią masową	- Maksymalny rozmiar pojedynczego wolumenu: 108 TB / 200 TB* <i>*wymagane co najmniej 32 GB pamięci RAM, tylko dla macierzy RAID 5 lub RAID 6</i> - Minimalny liczba wewnętrznych wolumenów: 1024 - Minimalny liczba obiektów iSCSI Target: 256 - Minimalny liczba jednostek iSCSI LUN: 512 - Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	- Minimalna liczba kont użytkowników lokalnych: 16 000 - Minimalna liczba grup lokalnych: 512 - Minimalna liczba folderów współdzielonych: 512 - Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 2 000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Chrome®, Firefox®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze; Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze)
Oprogramowanie	- Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych - Oprogramowanie zarządzające serwerem NAS

	musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów - Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. - Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Konserwacja	Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack dostarczonych z zestawem
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz.
Akcesoria	Przesuwanych szyn rack
Gwarancja	Wykonawca udzieli gwarancji: 5 lat na urządzenia główne 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack

6. Dyski twarde do serwera NAS – 8 sztuk

Minimalne wymagania:	
Pojemność	min. 8000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	Serial ATA III
Pamięć cache	min. 256 MB
Prędkość obrotowa	7200 obr./ min

7. UTM – 1 sztuka

Urządzenie typu UTM z 2 - letnim wsparciem.

Minimalne wymagania Zamawiającego	
Typ urządzenia	UTM
UTM (full scan) – przepustowość	1.18 Gbps
VPN (IMIX) - przepustowość	800 Mbps
Antywirus - przepustowość	1.47 Gbps
Interface 10/100/1000	8x1 Gb
Jednoczesne połączenia	3 500 000
Nowe połączenia na sekundę	34 000
VLAN	100
VPN typu site to site	IKEv2, IPSec, Policy and Route Based Tunnels, TLS hub
Opcje filtrowania	Browser Safe Search, Google for Business
Serwery proxy aplikacji	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3S, SMTPS, IMAPS, Explicit Proxy
Dynamiczny routing	RIP, OSPF, BGP
QoS	802.1Q, DSCP, IP Precedence
NAT	Statyczny, DHCP (server, client, relay), PPPoE, DynDNS

Zasilanie	Pojedynczy zasilacz -65W 90-264VAC~, 1.0A/1.5A 47-63Hz
Remote Access VPN	IKEv2, IPSec, L2TP, TLS

8. UPS – 2 sztuki

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	3000VA
2	Moc rzeczywista	3000W
3	Topologia (klasyfikacja IEC 62040-3)	Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC)
4	Sprawność przy pracy normalnej (100% obc.)	<94%
5	Sprawność w trybie podwyższonej sprawności (100% obc.)	>98%
6	Współczynnik mocy	1
7	Czas przełączenia na baterię	0 ms
8	Możliwość pracy równoległej	tak
9	Liczba, typ gniazd wyjściowych	8 gniazd IEC C13 (10A) + 2 gniazda IEC C19 (16A), w tym 2 zarządzalne grupy wraz z pomiarem zużytej energii
10	Typ gniazda wejściowego	1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW
11	Czas podtrzymania dla 100% obciążenia dla pf=1	3 min
12	Czas podtrzymania przy 50% obciążenia dla pf=1	10 min
13	Dodatkowe baterie	Możliwość dołożenia maksymalnie 4 zewnętrznych modułów bateryjnych
14	Napięcie znamionowe	200/208/220/230/240 V
15	Tolerancja napięci prostownika	176V – 276 V (100-276V przy <33% obciążeniu)
16	Częstotliwość znamionowa	50/60 Hz autodetekcja
17	Tolerancja częstotliwości	40– 70 Hz

18	Kształt napięcia	Sinusoidalny
19	Napięcie znamionowe wyjściowe	230 V (domyślnie) / możliwość wyboru 200/208/220/240 V
20	Zakres zmian napięcia	+/-1% napięcia nominalnego
21	Częstotliwość wyjściowa	50/60 Hz +/-0,5%
22	Współczynnik szczytu	3:1
23	Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
24	Baterie wymieniane przez użytkownika "na gorąco"	Tak
25	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
26	Ochrona przed głębokim rozładowaniem	Tak
27	Okresowy automatyczny test baterii	Tak
28	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
29	Zdolność zwarciova	90A
30	Możliwość uruchomienia bez napięcia w sieci	Tak
31	Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 6 szt.
32	Czas ładowania baterii do poziomu 90%	< 1,5 godz. do 90% pojemności użytkowej
33	Interfejs komunikacyjny	• USB • RS232 DB-9 żeński (HID) • 1 blok mini-zacisków dla zdalnego załączania/wyłączania • 1 blok mini-zacisków do zdalnego wyłączenia • 1 blok mini-zacisków przekaźnika wyjściowego

34	Panel sterowania z wyświetlaczem LCD	- Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii). - Poziomy rząd przycisków sterowania - Poziomy rząd wskaźników stanu : 4 LED - Sygnalizator akustyczny
35	Sygnały akustyczne	- Awaria - Niski stan naładowania baterii - Przeciążenie - Serwis
36	Przyciski sterujące i wskaźniki diodowe LED	- Przycisk Escape (anulowanie) - Przyciski funkcyjne (przewijanie w górę i w dół) - Przycisk Enter (potwierdzający) - Przycisk ON/OFF załączenia i wyłączenia - LED trybu zasilania z sieć i(kolor zielony) - LED trybu baterii (kolor żółty) - LED usterki (kolor czerwony) - LED w trybie obejścia (kolor pomarańczowy)
37	Kolor	Czarny RAL 9005
38	Typ obudowy	Uniwersalna Tower/Rack 2U
39	Wypożyczenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu 1 x kabel szeregowy RS-232 1 x kabel komunikacyjny USB 1 x kable wyjściowe IEC 16A 2 x kable wyjściowe IEC 10A uchwyty kablowe

		1 x zestaw szyn montażowych 19'
		podstawki do montażu wieżowego
40	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 - Citrix XEN 6.0
41	Zgodność ze standardem Energy Star	Tak
42	Maksymalna szerokość	440 mm
43	Maksymalna wysokość	86,5 mm
44	Maksymalna głębokość	605 mm
45	Maksymalny ciężar	27,4 kg
46	Poziom hałasu w odl. 1m	<47 dBA dla pracy normalnej
47	Znaki bezpieczeństwa	CE, C-Tick, IEC/EN 62040-1, IEC/EN 62040-2: Kat. C1, IEC/EN 62040-3
48	Gwarancja producenta	2 lata

9. Oprogramowanie do zarządzania bezpieczeństwem infrastruktury teleinformatycznej – 50 urządzeń.

Oprogramowanie dla 50 urządzeń wraz z wsparciem serwisowym na 5 lat.

1. Architektura / budowa

1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie.

1.2. Architektura / budowa:

1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.

- 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
- 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
- 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
- 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
- 1.3. Konfiguracja Architektury:
 - 1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
 - 1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

2. Wymagania systemowe

- 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
- 2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
 - 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2.
- 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
- 2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
- 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
- 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

- 3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- 3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL.
- 3.3. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

- 4.1. Funkcjonalność Klienta
 - 4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń

systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

4.3. Funkcjonalność panelu pracownika

4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

4.5. Wzorce aplikacji i pakietów

4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.

4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.

4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich połączeń.

4.7. Inwentaryzacja urządzeń sieciowych.

4.7.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.

4.8. Inwentaryzacja sprzętu.

4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.

4.9. Ochrona danych (DLP)

4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.

4.10. Szyfrowanie dysków wewnętrznych oraz zewnętrznych

4.10.1. System musi obsługiwać kompleksowe szyfrowanie dysków wewnętrznych i zewnętrznych USB, z wykorzystaniem BitLocker i różnych metod szyfrowania, takich jak XTS_AES_256 i AES_128. Musi umożliwiać zdalne zarządzanie procesem szyfrowania/desyfrowania, w tym masowe operacje na partycjach systemowych i niesystemowych, zarówno lokalnie, jak i zdalnie (poza NATem). Klucze szyfrujące są przechowywane i chronione w konsoli administracyjnej, dostępne tylko po uwierzytelnieniu administratora. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika i nie może być przez niego przerwany, z wyjątkiem stanów hibernacji i wyłączenia systemu, po których jest automatycznie kontynuowany.

4.11. Zdalna administracja komputerami

4.11.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.

4.12. System musi umożliwiać zdalne w technologii WEBRTC.

4.12.1. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednocześnie połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitem, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie.

4.13. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.14. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.15. Zdalne Zarządzanie Zaporą (Firewall)

4.15.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

4.16. Automatyzacja

- 4.16.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.
- 4.17. Zarządzanie magazynem IT
- 4.17.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
- 4.18. Repozytorium
- 4.18.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
- 4.19. Kody kreskowe
- 4.19.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
- 4.20. Wysyłanie wiadomości
- 4.20.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
- 4.21. System musi posiadać możliwość eksportu / importu treści.
- 4.22. Monitorowanie drukarek sieciowych i wydruków
- 4.22.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
- 4.23. Monitorowanie stron www
- 4.23.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
- 4.24. Monitorowanie serwerów WWW
- 4.24.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
- 4.25. Monitorowanie dziennika zdarzeń

- 4.25.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
- 4.26. System musi umożliwiać monitorowanie komunikatów Syslog.
- 4.27. Monitorowanie pracy komputerów
 - 4.27.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
- 4.28. Monitorowanie sensorów
 - 4.28.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
- 4.29. Repozytorium CMDB
 - 4.29.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
- 4.30. Worktime manager
 - 4.30.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.
- 4.31. Raportowanie i eksport danych
 - 4.31.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
- 4.32. System musi zapewnić interfejs API.
 - 4.32.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.
- 4.33. Powiadomienia
 - 4.33.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.
- 4.34. Bezpieczeństwo
 - 4.34.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

5. Wsparcie i pomoc

5.1.1. Pomoc techniczna

- 5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
- 5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
- 5.1.1.3. Czas trwania usługi SLA wynosi 60 miesięcy od dnia zakupu.